NEW YORK STATE
DEPARTMENT OF FINANCIAL SERVICES
ONE STATE STREET
NEW YORK, NEW YORK 10004

In the Matter of

NATIONAL SECURITIES CORPORATION

CONSENT ORDER

The New York State Department of Financial Services (the "Department" or "DFS") and National Securities Corporation ("National Securities" or the "Company") are willing to resolve the matters described herein without further proceedings.

WHEREAS, National Securities is licensed by the Department to sell life insurance, accident and health insurance, and variable life/variable annuities insurance in New York State.

WHEREAS, August 29, 2017 marked the effective date of New York's first-in-the nation cybersecurity regulation, 23 NYCRR 500 (the "Cybersecurity Regulation"). The Department's Cybersecurity Regulation is designed to address significant issues of cybersecurity and protect the financial services industry and consumers from the ever-increasing threat of data breaches and cyberattacks.

WHEREAS, the regulation's clearly defined standards for cooperative industry compliance, robust consumer data protection, vital cybersecurity controls, timely reporting of Cybersecurity Events, and enforcement were promulgated to strengthen cybersecurity and data

protection for industry and consumers.

WHEREAS, the Department has been investigating certain Cybersecurity Events, as defined by 23 NYCRR § 500.01(d), experienced within National Securities, as well as whether National Securities' cybersecurity program is in compliance with the Cybersecurity Regulation.

WHEREAS, based on the investigation, the Department has concluded that National Securities violated the following Cybersecurity Regulations: (1) National Securities' email environment, which accessed National Securities' internal network, did not have multi-factor authentication ("MFA") fully implemented for all users until August 14, 2020, and no reasonably equivalent or more secure access controls were approved in writing by the Company's Chief Information Security Officer ("CISO"), in violation of 23 NYCRR § 500.12(b); (2) certain third-party applications used by National Securities, which accessed National Securities' internal network or contained consumer Nonpublic Information ("NPI"), did not have MFA fully implemented as required, in violation of 23 NYCRR § 500.12(b); (3) National Securities failed to timely notify the Department of two cyber events that occurred in April 2018 and March 2019, both of which should have been timely reported to the Department, in violation of 23 NYCRR § 500.17(a); and (4) National Securities falsely certified compliance with the Cybersecurity Regulation for the calendar year 2018, in violation of 23 NYCRR § 500.17(b).

NOW THEREFORE, to resolve this matter without further proceedings pursuant to the Superintendent's authority under Section 408 of the New York Financial Services Law, the Department finds as follows:

THE DEPARTMENT'S FINDINGS

Introduction

1. The Department is the insurance regulator of the State of New York. The Superintendent of Financial Services is responsible for ensuring the safety and soundness of New York's insurance industry and promoting the reduction and elimination of fraud, abuse, and unethical conduct with respect to insurance participants.

2. The Superintendent has the authority to conduct investigations, bring enforcement proceedings, levy monetary penalties, and order injunctive relief against parties who have violated the relevant laws and regulations.

3. Among her many obligations to the public is the Superintendent's consumer protection function, which includes the protection of individuals' private and personally sensitive data from careless, negligent, or willful exposure by licensees of the Department.

4. To support this critical obligation, the Superintendent's Cybersecurity Regulation places on all DFS-regulated entities ("Covered Entities"[1]), including National Securities, an obligation to establish and maintain a cybersecurity program designed to protect the confidentiality and integrity of its Information Systems, as well as any consumer NPI[2] contained therein.

5. A "Cybersecurity Event" is an act or attempt, whether or not successful, to gain unauthorized access to information stored on an information system or disrupt or misuse such information system. 23 NYCRR 500.01(d). Licensees must file notice of a Cybersecurity Event with the Department pursuant to the requirements of 23 NYCRR 500.17(a)(1) and (a)(2). In

[1] The terms "Covered Entity" or "Covered Entities" used herein shall have the same definition as used in 23 NYCRR § 500.01(c).
[2] The terms "Nonpublic Information" or "NPI" used herein shall have the same definition as used in 23 NYCRR § 500.01(g).

particular, Part 500.17(a)(1) requires notice to the Superintendent, within 72 hours of determining there has been a Cybersecurity Event, when notices are "required to be provided to any government body, self-regulatory agency or any other supervisory body."

6. In addition to measures which require Covered Entities to report Cybersecurity Events to the Department (23 NYCRR § 500.17(a)) and to certify compliance with the Cybersecurity Regulation on an annual basis (23 NYCRR §500.17(b)), the Cybersecurity Regulation contains requirements to protect licensed entities' internal networks from threat actors seeking to access and exploit NPI (23 NYCRR § 500.12). Section 500.12 requires that Covered Entities implement multi-factor authentication ("MFA") when there is external access to a Covered Entity's internal network.[3] MFA requires more than one distinct authentication factor for successful access, such that a username and password alone are not sufficient to access an email account and its contents. MFA is the first line of defense against attempts to gain unauthorized access, including through phishing emails, which are emails sent by cyber criminals to deceive users into providing personal details or other confidential information to permit unauthorized access or harm to a protected information system.

Findings of Fact

The First Cybersecurity Event

7. National Securities reported a Cybersecurity Event to the Department on October 23, 2019 (the "First Cyber Event"). National Securities discovered the breach on September 18, 2019, when a Human Resources representative received a suspicious email from an employee requesting assistance with a change to the employee's direct deposit. The Human Resources

[3] The terms "multi-factor authentication" and "MFA" used herein shall have the same definition as used in 23 NYCRR § 500.01(f).

representative confirmed with the employee, via telephone, that she did not make the request and reported the incident to management.

8. National Securities' investigation of the First Cyber Event determined that the unauthorized access to the employee's Microsoft Office 365 ("O365") email account occurred from September 13, 2019 through September 18, 2019. The account was likely accessed through a phishing scheme.

9. The NPI of certain customers was potentially impacted. National Securities contacted all potentially impacted individuals, changed their account credentials to prevent unauthorized access, and provided credit monitoring.

10. At the time of the First Cyber Event, National Securities did not have MFA implemented for O365, as required by Section 500.12(b) of the Cybersecurity Regulation and was in the process of migrating users to a new Google Suite email platform, which is a collection of cloud computing, productivity and collaboration tools, software and products developed and marketed by Google, and which is now referred to as Google Workspace ("G Suite").

The Second Cybersecurity Event

11. National Securities reported a Cybersecurity Event to the Department on May 12, 2020 (the "Second Cyber Event"). National Securities discovered the Second Cyber Event on April 30, 2020, when an independent contractor, a broker, at one of National Securities' affiliates (National Asset Management, Inc., hereinafter "National Asset Management") noticed a potential unauthorized transfer of funds from a client account in the amount of $200,000. Following notification by the broker to his manager, two additional potential unauthorized transfers in the same amount were uncovered. Around the same time, the Help Desk Supervisor

detected that forwarding rules had been set up on the broker's O365 e-mail account for the time period of April 15, 2020 to April 30, 2020.

12. National Asset Management refunded the unauthorized transfers to the appropriate customers but did suffer a resulting loss of $400,000.

13. National Securities' investigation of the Second Cyber Event determined that the broker's O365 account was compromised from March 23, 2020 through April 30, 2020, and the compromise was likely the result of a phishing scheme.

14. The NPI of certain customers was potentially impacted. National Securities personally contacted all potentially impacted individuals, changed their account credentials to prevent unauthorized access, and provided credit monitoring.

15. At the time of the Second Cyber Event, while all National Securities corporate employees' accounts had been migrated to G Suite, with accompanying MFA controls, National Securities' affiliated independent contractors had not yet been migrated to G Suite.

Multi-factor Authentication on National Securities' Email Environment

16. Pursuant to Section 500.12(b) of the Cybersecurity Regulation, MFA must be utilized for any individuals accessing a Covered Entity's internal network from an external network. This requirement applies to third-party applications, including email platforms such as O365, that access a Covered Entity's internal network. Section 500.12(b) became effective on March 1, 2018.

17. As of March 1, 2018, National Securities' O365 platform, which was used by National Securities for email, did not have MFA implemented.

18. In or around August 2018, National Securities made the decision to migrate all user emails to G Suite, for which MFA would be enabled.

19. The migration to G Suite began in April 2019. National Securities completed the migration to G Suite for all corporate employees on November 26, 2019. However, the migration for independent contractors was not completed until August 14, 2020.

20. During the period between the effective date of Section 500.12(b) and the date MFA was fully implemented on National Securities' email environment, National Securities did have controls designed to protect the O365 environment.

21. These controls, however, fell short of the Section 500.12(b) standard of "reasonably equivalent or more secure access controls," which would have permitted National Securities to bypass the MFA requirement. Further, National Securities did not present sufficient evidence that these controls were approved in writing by the entity's CISO, as required by Section 500.12(b).

Multi-factor Authentication on National Securities' Third-Party Applications

22. In addition to its email environment, National Securities uses more than 60 third-party applications that contain NPI of National Securities' consumers and/or employees or have access to National Securities' internal network.

23. National Securities had not completed the MFA rollout for certain third-party applications as of the effective date of Section 500.12(b), and one application remained without MFA as of the date of this Consent Order. Although National Securities has access controls to reduce the risks associated with the remaining application, National Securities' CISO has not approved any "reasonably equivalent or more secure access controls" for these third-party applications.

Unreported Cyber Events

24. During the Department's investigation into National Securities' cybersecurity program, National Securities revealed that, in addition to the two Cybersecurity Events described above, National Securities was the victim of two additional Cybersecurity Events, which were not reported to the Department as promptly as possible and no later than 72 hours of their occurrence, as is required by 23 NYCRR § 500.17(a).

25. On April 12, 2018, National Securities' IT department identified emails from the Chief Financial Officer that were being forwarded by rule to an external account. After investigating, National Securities learned that the rule was set up by a threat actor who gained access to the O365 account because the Chief Financial Officer had clicked on a phishing email on April 3, 2018 (the "April 2018 Cyber Event").

26. National Securities concluded that certain customers had NPI potentially exposed.

27. National Securities reported the event to the Attorney General's Offices in New York, New Jersey, Connecticut, Massachusetts, as well as to all individuals who had their NPI potentially exposed. National Securities did not report the April 2018 Cyber Event to the Department as required by the Cybersecurity Regulation. National Securities changed account credentials to prevent unauthorized access and provided credit monitoring to all potentially impacted individuals.

28. The second unreported incident occurred when, on March 6, 2019, National Securities learned that an unauthorized threat actor gained access to an employee's secure document management system account, which is part of National Securities' professional tax software system (the "March 2019 Cyber Event"). After investigating, National Securities learned that the suspicious activity in the account began on December 1, 2018 and included

unauthorized access to the employee's O365 account. National Securities believes this incident was caused by a phishing scheme.

29. National Securities notified all potentially impacted customers of the breach, as well as the Internal Revenue Service, the United States Securities and Exchange Commission, the Federal Bureau of Investigation, and the local County Sheriff's Office. National Securities did not report the March 2019 Cyber Event to the Department as required by the Cybersecurity Regulation. National Securities changed account credentials to prevent unauthorized access and provided credit monitoring to all potentially impacted individuals.

Part 500 Compliance Certification

30. Pursuant to 23 NYCRR § 500.17(b), Covered Entities are required to annually certify their compliance with the Cybersecurity Regulation.

31. National Securities certified compliance with the Cybersecurity Regulation for the 2018 calendar year on January 23, 2019.

32. While National Securities timely certified compliance for the 2018 calendar year, due to the foregoing failures, National Securities was not in compliance with the Cybersecurity Regulation at the time of certification.

33. Thus, National Securities' filing of a Certification of Compliance, attesting to National Securities' compliance with the Cybersecurity Regulation for the 2018 calendar year, was false.

VIOLATIONS OF LAW AND REGULATIONS

34. The Company's email environment, which accessed the Company's internal network, did not fully implement MFA for all users until August 14, 2020, and no reasonably equivalent or more secure access controls were approved in writing by the Company's CISO, in

violation of 23 NYCRR § 500.12(b).

35. Certain third-party applications used by the Company, which accessed the Company's internal network or contained consumer NPI, did not have MFA fully implemented, and one application does not have MFA fully implemented, in violation of 23 NYCRR § 500.12(b).

36. The Company failed to timely notify the Department of the April 2018 Cyber Event, in violation of 23 NYCRR § 500.17(a).

37. The Company failed to timely notify the Department of the March 2019 Cyber Event, in violation of 23 NYCRR § 500.17(a).

38. The Company falsely certified compliance with the Cybersecurity Regulation for the calendar year 2018, in violation of 23 NYCRR § 500.17(b).

NOW THEREFORE, to resolve this matter without further proceedings, the Department and the Company stipulate and agree to the following terms and conditions:

SETTLEMENT PROVISIONS

Monetary Penalty

39. No later than ten (10) days after the Effective Date (as defined below) of this Consent Order, the Company shall pay a total civil monetary penalty pursuant to Financial Services Law § 408 to the Department in the amount of Three Million Dollars and 00/100 Cents ($3,000,000). The payment shall be in the form of a wire transfer in accordance with instructions provided by the Department.

40. The Company shall not claim, assert, or apply for a tax deduction or tax credit with regard to any U.S. federal, state, or local tax, directly or indirectly, for any portion of the civil monetary penalty paid pursuant to this Consent Order.

41. The Company shall neither seek nor accept, directly or indirectly, reimbursement or indemnification with respect to payment of the penalty amount, including but not limited to, payment made pursuant to any insurance policy.

42. In assessing a penalty for failures in cybersecurity compliance and required reporting, the Department has taken into account factors that include, without limitation: the extent to which the entity has cooperated with the Department in the investigation of such conduct, the gravity of the violations, and such other matters as justice and the public interest may require.

43. The Department acknowledges National Securities' commendable cooperation throughout this investigation. The Department also recognizes and credits National Securities' ongoing efforts to remediate the shortcomings identified in this Consent Order. Among other things, National Securities has demonstrated its commitment to remediation by devoting significant financial and other resources to enhance its cybersecurity program, including through changes now underway to its policies, procedures, systems, governance structures, and personnel.

Remediation

44. National Securities shall continue to strengthen its controls to protect its cybersecurity systems and the private data of consumers and shall, in accordance with the relevant provisions and definitions of 23 NYCRR § 500:

a. Cyber Security Incident Response Plan. Within one hundred twenty (120) days of the date of this Order, National Securities shall submit to the Department a comprehensive written Cybersecurity Incident Response Plan consistent with 23 NYCRR § 500.16. The Cybersecurity Incident Response Plan shall, at a minimum:

i. contain a plan designed to promptly respond to, and recover from, any Cybersecurity Event materially affecting the confidentiality, integrity or availability of National Securities' information systems or the continuing functionality of any aspect of National Securities' business or operations;

ii. codify the internal processes for responding to a Cybersecurity Event;

iii. address the goals of the Cybersecurity Incident Response Plan; define clear roles, responsibilities and levels of decision-making authority;

iv. provide a plan for external and internal communications and information sharing;

v. identify requirements for the remediation of any identified weaknesses in information systems and associated controls;

vi. address documentation and reporting regarding Cybersecurity Events and related incident response activities; and

vii. address the evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.

b. Cybersecurity Risk Assessment. Within one hundred twenty (120) days of the date of this Order, National Securities shall submit to the Department a comprehensive Cybersecurity Risk Assessment of its information systems consistent with 23 NYCRR § 500.09, which shall contain:

i. the reasonably necessary changes National Securities plans to implement to address any issues raised in the Cybersecurity Risk Assessment;

ii. any and all plans for revisions of controls to respond to technological developments and evolving threats, which shall consider the particular risks of National

Securities' business operations related to cybersecurity, NPI collected or stored, Information Systems utilized and the availability and effectiveness of controls to protect NPI and Information Systems;

iii. any and all plans for updating or creating written policies and procedures to include:

1. criteria for the evaluation and categorization of identified cybersecurity risks or threats facing National Securities;

2. criteria for the assessment of the confidentiality, integrity, security and availability of National Securities' information systems and NPI, including the adequacy of existing controls in the context of identified risks; and

3. requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the cybersecurity program will address the risk.

c. Training and Monitoring. Within one hundred twenty (120) days of the date of this Order, National Securities shall submit to the Department the following materials consistent with 23 NYCRR § 500.14:

i. its risk-based policies, procedures and controls designed to: (a) monitor the activity of Authorized Users and (b) detect unauthorized access or use of, or tampering with, NPI by such Authorized Users; and

ii. its most recent cybersecurity awareness training for all personnel, updated to reflect risks identified by National Securities in its Cybersecurity Risk Assessment.

Full and Complete Cooperation

45. The Company commits and agrees that it will fully cooperate with the Department regarding all terms of this Consent Order.

Waiver of Rights

46. The parties understand and agree that no provision of this Consent Order is subject to review in any court, tribunal, or agency outside of the Department.

47. The Company waives its right to further notice and hearing in this matter as to the allegations of past violations by the Department's Consumer Protection and Financial Enforcement Division up to and including the Effective Date of this Consent Order.

Parties Bound by the Consent Order

48. This Consent Order is binding on the Department and the Company, as well as any successors and assigns. This Consent Order does not bind any federal or other state agency or any law enforcement authority.

49. No further action will be taken by the Department against the Company or its successors for the conduct set forth in this Consent Order, or in connection with the remediation set forth in this Consent Order, provided that the Company fully complies with the terms of the Consent Order. Furthermore, no further action will be taken by the Department against the Company for conduct in connection with the Department's investigation, including, but not limited to, the MFA implementation issues with the Axos Clearing application through December 31, 2020.

50. Notwithstanding any other provision in this Consent Order, however, the Department may undertake additional action against the Company for transactions or conduct that was not disclosed in the written materials submitted to the Department in connection with this matter.

Breach of Consent Order

51. In the event that the Department believes the Company to be in material breach of the Consent Order, the Department will provide written notice to the Company, and the Company must, within ten (10) days of receiving such notice, or on a later date if so determined in the Department's sole discretion, appear before the Department to demonstrate that no material breach has occurred or, to the extent pertinent, that the breach is not material or has been cured.

52. The Company understands and agrees that its failure to make the required showing within the designated time period shall be presumptive evidence of the Company's breach. Upon a finding that a breach of this Consent Order has occurred, the Department has all the remedies available to it under the New York Insurance and Financial Services Laws, and any other applicable laws, and may use any evidence available to the Department in any ensuing hearings, notices, or orders.

Notices

53. All notices or communications regarding this Consent Order shall be sent to:

For the Department:

Terri-Anne S. Caplan
Senior Assistant Deputy Superintendent for
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
One State Street
New York, NY 10004

Madeline W. Murphy
Assistant Deputy Superintendent for
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
One Commerce Plaza
Albany, NY 12257

Tatsiana Zhuk
Special Assistant to the Executive Deputy Superintendent for
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
One State Street
New York, NY 10004

For National Securities Corporation:

Fred Knopf
General Counsel
200 Vesey Street
25th Floor
New York, NY 10281

Brian Mahanna
Wilmer Cutler Pickering Hale & Dorr
250 Greenwich Street
New York, NY 10007

Miscellaneous

54. This Consent Order and any dispute thereunder shall be governed by the laws of the State of New York without regard to any conflicts of laws principles.

55. This Consent Order may not be altered, modified, or changed unless in writing and signed by the parties hereto.

56. This Consent Order constitutes the entire agreement between the Department and the Company and supersedes any prior communication, understanding, or agreement, whether written or oral, concerning the subject matter of this Consent Order.

57. Each provision of this Consent Order shall remain effective and enforceable against the Company, its successors, and assigns, until stayed, modified, suspended, or terminated by the Department.

58. In the event that one or more provisions contained in this Consent Order shall for any reason be held to be invalid, illegal, or unenforceable in any respect, such invalidity, illegality, or unenforceability shall not affect any other provision of this Consent Order.

59. No promise, assurance, representation, or understanding other than those contained in this Consent Order has been made to induce any party to agree to the provisions of this Consent Order.

60. Nothing in this Consent Order shall be construed to prevent any consumer from pursuing any right or remedy at law.

61. Except with regard to the enforcement of this Consent Order, the Company's consent to the provisions of this Consent Order does not bar, estop, waive, or otherwise prevent the Company from raising any defenses to any action taken by any federal or state agency or department, or any private action against the Company.

62. This Consent Order may be executed in one or more counterparts, and shall become effective when such counterparts have been signed by each of the parties hereto (the "Effective Date").

[*remainder of this page intentionally left blank*]

IN WITNESS WHEREOF, the parties have caused this Consent Order to be signed on the dates set forth below.

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES

By: /s
DESIREE S. MURNANE
Senior Assistant Deputy Superintendent for Consumer Protection and Financial Enforcement

April 12, 2021

By: /s
CHRISTOPHER B. MULVIHILL
Deputy Superintendent for Consumer Protection and Financial Enforcement

April 12, 2021

By: /s
KATHERINE A. LEMIRE
Executive Deputy Superintendent for Consumer Protection and Financial Enforcement

April 12, 2021

NATIONAL SECURITIES CORPORATION

By: /s
FRED KNOPF
General Counsel

April 9, 2021

THE FOREGOING IS HEREBY APPROVED. IT IS SO ORDERED.

/s
LINDA A. LACEWELL
Superintendent of Financial Services

April 12, 2021